PART 9—SECURITY INFORMATION REGULATIONS

AUTHORITY: E.O. 13526 (75 FR 707, January 5, 2010); Information Security Oversight Office Directive 32 CFR part 2001 (75 FR 37254, June 28, 2010).

SOURCE: 79 FR 35936, June 25, 2014, unless otherwise noted.

§ 9.1 Basis.

The regulations in this part, taken together with 32 CFR part 2001 and Volume 5 of the Department's Foreign Affairs Manual, provide the basis for the security classification program of the U.S. Department of State (''the Department'') implementing Executive Order 13526 on Classified National Security Information (''the Executive Order'' or ''the Order'').

§ 9.2 Objective.

The objective of the Department's classification program is to ensure that national security information is protected from unauthorized disclosure, but that it remains classified only to the extent and for such a period as is necessary.

§ 9.3 Senior agency official.

The Executive Order requires that each agency that originates or handles classified information designate a Senior Agency Official to direct and administer its information security program. The Department's senior agency official is the Under Secretary of State for Management. The Senior Agency Official is assisted in carrying out the provisions of the Executive Order and the Department's information security program by the Assistant Secretary for Diplomatic Security, the Assistant Secretary for Administration, and the Deputy Assistant Secretary for Global Information Services.

§ 9.4 Original classification.

(a) *Definition.* Original classification is the initial determination that certain information requires protection against unauthorized disclosure in the interest of national security (*i.e.*, national defense or foreign relations of the United States), together with a designation of the level of classification.

(b) *Classification levels.* (1) Top Secret shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

(2) Secret shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) Confidential shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(c) *Classification requirements and considerations.* (1) Information may not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security in accordance with section 1.2 of the Executive Order, and it pertains to one or more of the following:

(i) Military plans, weapons systems, or operations;

(ii) Foreign government information;

(iii) Intelligence activities (including covert action), intelligence sources or methods, or cryptology;

(iv) Foreign relations or foreign activities of the United States, including confidential sources;

(v) Scientific, technological, or economic matters relating to the national security;

(vi) United States Government programs for safeguarding nuclear materials or facilities;

(vii) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or

(viii) The development, production, or use of weapons of mass destruction.

(2) In classifying information, the public's interest in access to government information must be balanced against the need to protect national security information.

(3) The unauthorized disclosure of foreign government information is presumed to cause damage to national security.

(d) *Classification limitations and prohibitions.* (1) In no case shall information be classified in order to conceal violations of law, inefficiency, or administrative error, or to prevent embarrassment to a person, organization, or agency, to restrain competition, or to prevent or delay the release of information that does not require protection in the interest of the national security.

(2) A reference to classified documents that does not directly or indirectly disclose classified information may not be classified or used as a basis for classification.

(3) Only information owned by, produced by or for, or under the control of the U.S. Government may be originally classified.

(e) *Duration of classification.* (1) Information shall be classified for as long as is required by national security considerations, subject to the limitations set forth in section 1.5 of the Executive Order. When it can be determined, a specific date or event for declassification in less than 10 years shall be set by the original classification authority at the time the information is originally classified. If a specific date or event for declassification cannot be determined, information shall be marked for declassification 10 years from the date of the original decision, unless the original classification authority determines that the sensitivity of the information requires that it be marked for declassification for up to 25 years from the date of the original decision except for:

(i) Information that would reveal the identity of a confidential human source or a human intelligence source, or key design concepts of weapons of mass destruction, in which case the duration of classification shall be up to 75 years and shall be designated with the markings ''50X1–HUM'' and ''50X2–WMD,'' respectively; and

(ii) Specific information incorporated into the classification guide under section 2.2(e) of the Executive Order relating to exemptions from automatic declassification.

(2) An original classification authority may extend the duration of classification up to 25 years from the date of origin of the document, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under the Executive Order are met.

(3) No information may remain classified indefinitely. Information marked for an indefinite duration of classification under predecessor orders, such as ''Originating Agency's Determination Required'' (OADR) or classified information that contains incomplete declassification instructions or lacks declassification instructions, shall be declassified in accordance with Part 3 of the Order.

§ 9.5 Original classification authority.

(a) Authority for original classification of information as Top Secret may be exercised by the Secretary and those officials delegated this authority in writing by the Secretary. Such authority has been delegated to the Deputy Secretaries, the Under Secretaries, the Counselor, Assistant Secretaries and equivalents; Chiefs of Mission and U.S. representatives to international organizations; and certain other officers within the Department and at posts abroad.

(b) Authority for original classification of information as Secret or Confidential may be exercised only by the Secretary, the Senior Agency Official, and those officials delegated this authority in writing by the Secretary or

the Senior Agency Official. Such authority has been delegated to Deputy Assistant Secretaries, Principal Officers at consulates general and consulates abroad, and certain other officers within the Department and at posts abroad. In the absence of the Secret or Confidential classification authority, the person designated to act for that official may exercise that authority.

§ 9.6 Derivative classification.

(a) *Definition.* Derivative classification is: the incorporating, paraphrasing, restating, or generating in new form information that is already classified and the marking of the new material consistent with the classification of the source material, or the marking of the information in accordance with an authorized classification guide. Duplication or reproduction of existing classified information is not derivative classification. Persons who apply classification markings derived from source material or as directed by a classification guide need not possess original classification authority.

(b) *Responsibility.* Information classified derivatively from other classified information shall be classified and marked in accordance with instructions from an authorized classifier or in accordance with an authorized classification guide and shall comply with the standards set forth in sections 2.1–2.2 of the Executive Order and 32 CFR 2001.22. The duration of classification of a document classified by a derivative classifier using a classification guide shall not exceed 25 years except for:

(1) Information that would reveal the identity of a confidential human source or a human intelligence source (50X1–HUM) or key design concepts of weapons of mass destruction (50X2–WMD), and

(2) Specific information incorporated into the classification guide under section 2.2(e) of the Executive Order relating to exemptions from automatic declassification.

(c) *Department of State Classification Guide.* The Department of State Classification Guide (DSCG) is the primary authority for the classification of information in documents created by Department of State personnel. The Guide is classified ''Confidential'' and is found on the Department of State's classified Web site.

§ 9.7 Identification and marking.

(a) Classified information shall be marked pursuant to the standards set forth in section 1.6 of the Executive Order, 32 CFR part 2001, subpart C, and internal Department guidance in 5 Foreign Affairs Manual.

(b) Foreign government information shall retain its original classification markings or be marked and classified at a U.S. classification level that provides a degree of protection at least equivalent to that required by the entity that furnished the information. Foreign government information retaining its original classification markings need not be assigned a U.S. classification marking provided the responsible agency determines that the foreign government markings are adequate to meet the purposes served by U.S. classification markings.

(c) Information assigned a level of classification under predecessor executive orders shall be considered as classified at that level of classification despite the omission of other required markings.

(d) Prior to public release, all declassified records shall be appropriately marked to reflect their declassification.

§ 9.8 Classification challenges.

(a) *Challenges.* Authorized holders of information pertaining to the Department of State who believe that its classification status is improper are expected and encouraged to challenge the classification status of the information. Such persons making challenges to the classification status of information shall not be subject to retribution for such action. Informal, usually oral, challenges are encouraged. Formal challenges to classification actions shall be in writing to an original classification authority (OCA) with jurisdiction over the information and a copy of the challenge shall be sent to the Office of Information Programs and Services (IPS) of the Department of State, SA–2, 515 22nd St. NW., Washington, DC 20522–8100. The Department (either the

OCA or IPS) shall provide an initial response in writing within 60 calendar days.

(b) *Appeal procedures and time limits.* A negative response may be appealed to the Department's Appeals Review Panel (ARP) and should be sent to: Chairman, Appeals Review Panel, c/o Director, Office of Information Programs and Services/Appeals Officer, at the IPS address given above. The appeal shall include a copy of the original challenge, the response, and any additional information the appellant believes would assist the ARP in reaching its decision. The ARP shall respond within 90 calendar days of receipt of the appeal. A negative decision by the ARP may be appealed to the Interagency Security Classification Appeals Panel (ISCAP) referenced in section 5.3 of Executive Order 13526. If the Department fails to respond to a formal challenge within 120 calendar days or if the ARP fails to respond to an appeal within 90 calendar days, the challenge may be sent directly to the ISCAP.

(c) *Pre-publication review materials.* The provisions for classification challenges do not apply to material required to be submitted for pre-publication review, or other administrative action, pursuant to a non-disclosure agreement.

§9.9 Declassification and downgrading.

(a) *Declassification processes.* Declassification of classified information may occur:

(1) After review of material in response to a Freedom of Information Act (FOIA) request, mandatory declassification review request, discovery request, subpoena, classification challenge, or other information access or declassification request;

(2) After review as part of the Department's systematic declassification review program;

(3) As a result of the elapse of the time or the occurrence of the event specified at the time of classification;

(4) By operation of the automatic declassification provisions of section 3.3 of the Executive Order with respect to material more than 25 years old.

(b) *Downgrading.* When material classified at the Top Secret level is reviewed for declassification and it is determined that classification continues to be warranted, a determination shall be made whether downgrading to a lower level of classification is appropriate. If downgrading is determined to be warranted, the classification level of the material shall be changed to the appropriate lower level.

(c) *Authority to downgrade and declassify.* (1) Classified information may be downgraded or declassified by:

(i) The official who originally classified the information if that official is still serving in the same position and has original classification authority;

(ii) A successor in that capacity if that individual has original classification authority;

(iii) A supervisory official of either if the supervisory official has original classification authority;

(iv) Other Department officials specifically delegated declassification authority in writing by the Secretary or the Senior Agency Official; or

(v) The Director of the Information Security Oversight Office pursuant to Sec. 3.1(a) of E.O. 13526.

(2) The Department shall maintain a record of Department officials specifically designated as declassification and downgrading authorities.

(d) *Declassification in the public interest.* Although information that continues to meet the classification criteria of the Executive Order or a predecessor order normally requires continued protection, in some exceptional cases the need to protect information may be outweighed by the public interest in disclosure of the information. When such a question arises, it shall be referred to the Secretary or the Senior Agency Official for decision on whether, as an exercise of discretion, the information should be declassified and disclosed. This provision does not amplify or modify the substantive criteria or procedures for classification or create any substantive or procedural right subject to judicial review.

(e) *Public disclosure of declassified information.* Declassification of information is not, by itself, authorization for its public disclosure. Previously classified information that is declassified may be exempt from public disclosure under the FOIA, the Privacy Act, or

various statutory confidentiality provisions. There also may be treaties or other international agreements that would preclude public disclosure of declassified information.

§ 9.10 Mandatory declassification review

(a) *Scope.* All information classified under E.O. 13526 or predecessor orders shall be subject to mandatory declassification review upon request by a member of the public or a U.S. government employee or agency with the following exceptions:

(1) Information originated by the incumbent President or the incumbent Vice President; the incumbent President's White House staff or the incumbent Vice President's staff; committees, commissions, or boards appointed by the incumbent President; other entities within the Executive Office of the President that solely advise and assist the incumbent President;

(2) Information that is the subject of pending litigation; and

(3) Information that has been reviewed for declassification within the past two years which need not be reviewed again, but the requester shall be given appeal rights.

(b) *Requests.* Requests for mandatory declassification review should be addressed to the Office of Information Programs and Services, U.S. Department of State, SA–2, 515 22nd St. NW., Washington, DC 20522–8100.

(c) *Description of information.* In order to be processed, a request for mandatory declassification review must describe the document or the material containing the information sought with sufficient specificity to enable the Department to locate the document or material with a reasonable amount of effort. Whenever a request does not sufficiently describe the material, the Department shall notify the requester that no further action will be taken unless additional description of the information sought is provided.

(d) *Refusal to confirm or deny existence of information.* The Department may refuse to confirm or deny the existence or nonexistence of requested information whenever the fact of existence or nonexistence is itself classified.

(e) *Processing.* In responding to mandatory declassification review requests, the Department shall make a review determination as promptly as possible, but in no case more than one year from the date of receipt of the request, and notify the requester accordingly. When the requested information cannot be declassified in its entirety, the Department shall release all meaningful portions that can be declassified and that are not exempt from disclosure on other grounds.

(f) *Other agency information.* When the Department receives a request for information in its possession that was originally classified by another agency, it shall refer the request and the pertinent information to the other agency unless that agency has agreed that the Department may review such information for declassification on behalf of that agency. In any case, the Department is responsible for responding to the requester with regard to any responsive information, including other-agency information, unless a prior arrangement has been made with the originating agency.

(g) *Foreign government information.* In the case of a request for material containing foreign government information, the Department shall determine whether the information may be declassified and may, if appropriate, consult with the relevant foreign government on that issue. If the Department is not the agency that initially received the foreign government information, it may consult with the original receiving agency.

(h) *Documents or material containing RD or Transclassified Foreign Nuclear Information (TFNI).* Documents or material containing RD or TFNI will be submitted to DOE for review. Documents containing FRD will be submitted to DOE or DoD for review.

(i) *Appeals.* Any denial of a mandatory declassification review request may be appealed to the ARP. A denial by the ARP of a mandatory declassification review appeal may be further appealed to the ISCAP. A failure of the Department to make a determination on a mandatory declassification review request within one year from the date of its receipt or to respond to an appeal

of a denial by the ARP within 180 calendar days of its receipt may be appealed directly to the ISCAP.

§9.11 Systematic declassification review.

The Director of the Office of Information Programs and Services shall be responsible for conducting a program for systematic declassification review of historically valuable records that: were exempted from the automatic declassification provisions of section 3.3 of the Executive Order; or will soon become subject to the automatic declassification provisions of section 3.3 of the Order. The Director shall prioritize such review in accordance with priorities established by the National Declassification Center.

§9.12 Sharing other-agency classified information.

The long-standing third-agency rule has required prior originating agency approval before a receiving agency could further disseminate classified information. Under the Executive Order, unless the originating agency indicates on the material that prior approval is required and provided that the criteria for access under section 4.1(a) of the Order are met, a receiving agency may further disseminate classified information in documents created subsequent to the effective date of the Order to another agency or U.S. entity without consultation with the originating agency. ''U.S. entity'' includes cleared state, local, tribal, and private sector entities. Similarly, under certain circumstances, receiving agencies may pass such classified information to foreign governments.

§9.13 Access to classified information by historical researchers and certain former government personnel.

(a) The restriction in E.O. 13526 and predecessor orders on limiting access to classified information to individuals who have a need-to-know the information may be waived, under the conditions set forth below, for persons who: are engaged in historical research projects; have served as President or Vice President; have occupied senior policy-making positions in the Department of State or other U.S. government agencies to which they were appointed or designated by the President or the Vice President. It does not include former Foreign Service Officers as a class or persons who merely received assignment commissions as Foreign Service Officers, Foreign Service Reserve Officers, Foreign Service Staff Officers, and employees.

(b) Requests by such persons must be submitted in writing to the Office of Information Programs and Services at the address set forth above and must include a general description of the records sought, the time period covered by the records that are the subject of the request, and an explanation why access is sought. Requests for access by such requesters may be granted if:

(1) The Secretary or the Senior Agency Official determines in writing that access is consistent with the interests of national security;

(2) The requester agrees in writing to safeguard the information from unauthorized disclosure or compromise;

(3) The requester submits a statement in writing authorizing the Department to review any notes and manuscripts created as a result of access;

(4) The requester submits a statement in writing that any information obtained from review of the records will not be disseminated without the express written permission of the Department;

(c) If a requester uses a research assistant, the requester and the research assistant must both submit a statement in writing acknowledging that the same access conditions set forth in paragraphs (b)(2) through (b)(4) of this section apply to the research assistant. Such a research assistant must be working for the applicant and not gathering information for publication on his or her own behalf.

(d) Access granted under this section shall be limited to items the official originated, reviewed, signed, or received while serving as a Presidential or Vice Presidential appointee or designee or as President or Vice President.

(e) Such requesters may seek declassification and release of material to which they have been granted access under this section through either the

FOIA or the mandatory declassification review provisions of E.O. 13526. Such requests shall be processed in the order received, along with other FOIA and mandatory declassification review requests, and shall be subject to the fees applicable to FOIA requests.

§ 9.14 Pre-publication review of writings by former Department personnel.

The Department provides pre-publication review of writings on foreign relations topics by former Department personnel, including contractors and detailees, who had security clearances to try to ensure that former personnel do not violate their agreements on non-disclosure of classified national security information in such writings. Manuscripts (including articles, speeches, books, etc.) should be sent to the Director, Office of Information Programs and Services, 515 22nd St. NW., Washington, DC 20522–8100. Questions about pre-publication clearance may be sent to *Classification@state.gov*.

§ 9.15 Assistance to the Historian's Office.

All elements of the Department shall assist the Historian's Office in its preparation of the Foreign Relations of the United States (FRUS) series such as by providing prompt access to and, when possible, declassification of information deemed appropriate for inclusion in the FRUS.

§ 9.16 Safeguarding.

Specific controls on the use, processing, storage, reproduction, and transmittal of classified information within the Department to provide protection for such information and to prevent access by unauthorized persons are contained in Volume 12 of the Department's Foreign Affairs Manual.

PART 9a—SECURITY INFORMATION REGULATIONS APPLICABLE TO CERTAIN INTERNATIONAL ENERGY PROGRAMS; RELATED MATERIAL

Sec.

AUTHORITY: E.O. 11932 (41 FR 32691), E.O. 11652 (37 FR 5209, National Security Council Directive of May 17, 1972 (37 FR 10053).

SOURCE: 42 FR 46516, Sept. 16, 1977; 42 FR 57687, Nov. 4, 1977, unless otherwise noted.

§ 9a.1 Security of certain information and material related to the International Energy Program.

These regulations implement Executive Order 11932 dated August 4, 1976 (41 FR 32691, August 5, 1976) entitled ''Classification of Certain Information and Material Obtained from Advisory Bodies Created to Implement the International Energy Program.''

§ 9a.2 General policy.

(a) The United States has entered into the Agreement on an International Energy Program of November 18, 1974, which created the International Energy Agency (IEA). This program is a substantial factor in the conduct of our foreign relations and an important element of our national security. The effectiveness of the Agreement depends significantly upon the provision and exchange of information and material by participants in advisory bodies created by the IEA. Confidentiality is essential to assure the free and open discussion necessary to accomplish the tasks assigned to those bodies.

(b) These regulations establish procedures for the classification, declassification, storage, access, and dissemination of certain information related to the International Energy Program.

§ 9a.3 Scope.

These regulations apply to all information and material classified by the United States under the provisions of E.O. 11932, dated August 4, 1976 entitled ''Classification of Certain Information and Material Obtained From Advisory Bodies Created To Implement The International Energy Program.''